Anthem: Hackers tried to breach system as early as Dec. 10

February 7 2015, byBrandon Bailey

In this Feb. 5, 2015 file photo, the Anthem logo hangs at the health insurer's corporate headquarters in Indianapolis. Insurers aren't required to encrypt consumers' data under a 1990s federal law that remains the foundation for health care privacy in the Internet age _ a striking omission in light of the cyberattack against Anthem, the nation's second-largest health insurer. (AP Photo/Michael Conroy, File)

(AP)—The hackers who stole millions of health insurance records from

Anthem Inc. commandeered the credentials of five different employees while seeking to penetrate the company's computer network—and they may have been inside the system since December.

Anthem said this week that hackers stole names, Social Security numbers and other sensitive information for up to 80 million Anthem customers, in a breach that was first detected on Jan. 27. That's when an Anthem computer system administrator discovered outsiders were using his own security credentials to log into the company system and steal data.

Investigators now believe the hackers somehow compromised the credentials of five different tech workers, possibly through some kind of "phishing" scheme that could have tricked a worker into unknowingly revealing a password or downloading malicious software.

The company also confirmed Friday that it found that unauthorized data queries with similar hallmarks started as early as Dec. 10 and continued sporadically until Jan. 27. Attempts may also have been made earlier in 2014, said Kristin Binns, a spokeswoman for Indianapolis-based Anthem, the nation's second-largest health insurer.

Those earlier attempts, including the one on Dec. 10, were deflected by the company's network security defenses, Binns said. Like most companies, Anthem routinely deflects a variety of attempts to make unauthorized access to its systems, she added.

The hackers succeeded in penetrating the system and stealing customer data sometime after Dec. 10 and before Jan. 27, Binns said. She declined to be more specific, saying the matter is still under investigation. Binns was confirming details of an Anthem corporate email that was first made public by an industry blog, CSO Online.

Experts say it's not unusual for sophisticated hacking groups to make repeated attempts to penetrate a computer system before they succeed.

"They may try to compromise them every single day, until the company makes a mistake or one individual makes a mistake," said Jaime Blasco, lab director at AlienVault, a Silicon Valley cyber-security firm that has investigated other hacking attempts but is not involved in the Anthem case.

Anthem's security consultants have said the breach resulted from a "sophisticated" attack by hackers using techniques usually associated with organized financial crime rings or groups working for the government of some country. Blasco said that appears likely.

"This is not some amateur that's trying to hack into their system. We are talking about professionals," he said.

Meanwhile, Anthem warned Friday that other scammers are targeting current and former customers with "phishing" emails that seek to capitalize on concern over the massive data breach. The emails invite customers to enroll in free credit monitoring by clicking on a link, which the company said is a trick aimed at stealing customers' personal information.

"There is no indication that the scam email campaigns are being conducted by those that committed the cyberattack, or that the information accessed in the attack is being used by the scammers," the company said in a statement.

https://phys.org/news/2015-02-anthem-hackers-breach-early-dec.html